State of North Carolina
Office of the State Controller

Michael F. Easley, Governor

David McCoy, State Controller

October 1, 2008

<u>**MEMORANDUM**</u>

TO: Agency Fiscal Officers
     University Vice Chancellors
     Community College Business Officers
     Local Units of Government Finance Officers

FROM: David T. McCoy

SUBJECT: PCI Data Security Compliance Policy

Under a master services agreement with SunTrust Merchant Services (STMS), eligible entities (agencies, universities, community colleges, and local units of government) are able to subscribe to merchant card processing services. The Office of the State Controller (OSC) functions as "facilitator" of the separate and individual arrangements made between participating entities and STMS.

Contractually, each participating entity is separately and individually responsible for adhering to the requirements of the MSA, which includes becoming and remaining compliant with the PCI Data Security Standard (PCI DSS), a requirement of the card associations. The primary focus of the standard is to help merchants improve the safekeeping of cardholder information by tightening their overall security standards, which in turn reduces their chances of experiencing security breaches, fraud, and potential catastrophic financial losses. Merchants found to be non-compliant with the PCI DSS are subject to substantial fines and penalties, as well as subject to having their merchant card services being terminated by STMS.

On June 19, 2008, the OSC announced changes in the compliance validation service being obtained through our vendor, Trustwave. The transition to the new process is nearly complete. To finalize the transition, the OSC has issued a policy to govern the ongoing compliance requirements. The policy, entitled "Compliance with PCI Data Security Standards," can be viewed at the following link:
http://www.ncosc.net/SECP/Compliance_with_PCI_Data_Security_Standards.pdf

The policy addresses the situation where a participant may be deemed non-compliant with the standard, as detected through the Trustwave compliance validation service. The policy also incorporates the involvement of central oversight agencies. All participants should review this policy and take the necessary action to ensure compliance with the standards. To assist your agency in this endeavor, please review the document, "Responding to Notice of Non-Compliance", which is located at the following hyper link:
http://www.ncosc.net/programs/risk_mitigation_pci.html

Any questions may be addressed to OSC's Support Services Center, telephone (919) 875-HELP (4357).